IDNewswire®
Trends in Personal Identification and Biometrics
www.cardtechnology.com Vol. 4 No. 2 January 28, 2005

Health Care CIO Tests Implantable Identification Chip Pg. 6
John Halamka, M.D., will always have a chip on his shoulder. The CIO at Boston's CareGroup Healthcare System, is the first volunteer to test an implantable radio frequency identification chip for medical use.

User Name And Passwords Still Reign In Health Care

A doctor walks up to a clerk in a large warehouse and asks for a patient's medical record. The clerk disappears for a second and reappears with the correct information. When another doctor approaches, the clerk knows what information the doctor wants before he asks for it.

This television commercial touts the benefits of medical records electronically being available at a doctor's fingertips on a moment's notice. In real life, a patient's records are more likely to be readily available if the patient seeks care at a hospital they normally visit; obtaining those files is likely to be more problematic if it's the first time or an emergency visit.

To remedy these problems, President Bush over the past year has been touting health care modernization and the development of a national health information network. The goal is for a patient's health records to be accessible anywhere at any time, no matter the institution. At the same time as hospital IT administrators consider how to build these networks, they know they are also required to ensure the security and integrity of electronic health data under the Health Insurance Portability and Accountability Act.

These twin goals of accessibility and privacy are on a collision course. As a national network emerges, safeguards will have to be put in place to make sure only authorized individuals are able to access patient information. It's too early to know which authentication technologies will be used. For HIPAA compliance, some health care providers are using such high-tech security methods as smart cards, biometrics and radio frequency IDs. Smart cards may also find their way into the hands of patients as tools for tracking medical information and prescriptions.

But for employee authentication, user name and password is still the most common choice, says Carol Quinsey, professional practice manager at the American Health Information Management Association, a Chicago-based organization that specializes in educating health care IT workers. HIPAA requires that passwords be secure, typi-

> Passwords, Page 2

Fingerprint Images May Be Stored On Government IDs

The standard identification card for U.S. government employees and contractors could possibly store two fingerprint images from the cardholder as opposed to the digital representations of finger images known as templates. That is raising concerns about privacy, as it opens the door to an individual's actual fingerprints being stolen from the card and misused.

The National Institute of Standards and Technology, the U.S. Commerce Department's research agency, says images should be used because there is no guarantee that a template derived by one vendor will be usable with another vendor's system. Images should work with scanners and matching algorithms from any supplier, according to a document released by the agency on Monday.

"We don't know if templates are interchangeable," says Charles Wilson, manager of the image group at NIST's Information Technology Lab and coauthor of the new specification. "This is the only thing we know that guarantees interoperability."

This proposal for the standard identification card being developed for federal workers and contractors

> Images, Page 4

Fingerprints On The Menu At School Cafeterias

Kids forget stuff. House keys, ID cards and lunch money are all likely to be left behind as kids run off to school in the morning.

This potentially causes a problem when lunchtime rolls around and little Timmy or Tammy doesn't have money for a meal. To solve this problem, some schools around the country are using biometric scanners in cafeterias, says Brian Wong, a consultant at the New York-based International Biometric Group, a consulting and research firm.

Biometrics help schools speed up lunch lines, limit fraud and bullying, and improve the U.S. government's National School Lunch Program, says Mitch Johns, president of Altoona, Pa.-based Food Service Solutions, a company that provides payments systems to educational institutions.

Food Service Solutions has installed its fingerprint payments system at 40 schools with 250,000 students, Johns says. "The goal is no cash in the lunch line," he says.

An added benefit is the funding schools receive for the National School Lunch Program, which allows children from low-income families to receive free or discounted meals. By requiring all children to use biomet-

> Menu, Page 5

IBG: Biometrics And Mobile Phones

As cell phones become more feature-rich and essential to our daily lives, the importance of securing these devices becomes more important. Increasingly financial transactions are conducted on cell phones, thus necessitating some form of user authentication. For these reasons biometric utilization has been and will be a relevant force in the cell phone industry.

> IBG, Page 7

> Passwords, Page 1

cally more than seven characters and a mix of letters and numbers, she says. The passwords also must be changed every 90 days.

Because these passwords are hard to remember, doctors and nurses often write them down somewhere they can easily be found. At one hospital Quinsey visited, "the nursing staff would write it down and tape them to the back of the badges. You would walk into the lounge and there would be all these badges with passwords on them."

Single sign-on, an application that would provide a single user name and password for log-on to all applications, is one way out. But vendors have yet to provide a product that offers seamless integration between multiple medical software programs, Quinsey says. Using biometrics or smart cards with simpler passwords are two other potential solutions, but neither has been widely adopted, Quinsey says.

Biometric technologies face some obstacles in the health care field, Quinsey says. Fingerprints, the most tested biometrics, are problematic because hospital employees often wear gloves. Also, the powder from the gloves dries out the hand making it more difficult to get a reliable match, she says. Iris is an alternative but the cameras are expensive.

'You would walk into the lounge and there would be all these badges with passwords on them. The nursing staff would write it down and tape them to the back of the badges.'
— Carol Quinsey, AHIMA

Cupertino, Calif.-based Oblix Inc. has provided identity management software to 200 customers, including Ontario, Canada's Smart Systems for Health Agency, a government agency that is working to electronically connect doctors, hospitals, laboratories, public health offices, community care access centers and pharmacies.

Oblix provides the ID software that allows 150,000 health care providers at 24,000 organizations in Ontario to securely access Web sites and patient information, says Prakash Ramamurthy, vice president of products and technology at Oblix. This includes a user authentication system to make sure only authorized professionals have access to the information. Oblix also provides auditing capabilities so the sites can be monitored for security and unauthorized access.

The system provides health care practitioners with a single user name and password for the following resources: secure e-mail for exchanging patient information; a portal providing health news, alerts and a drug database; and a common form to collect data from patients who receive care at multiple facilities.

A typical user of the Smart Systems for

> Passwords, Page 3

> **Passwords,** Page 2

Health Agency site uses a user name and password for access, Ramamurthy says. But about 10% of the time a second form of authentication, such as a smart card or biometric, is used for access to more secure areas of the site. "We find a combination of user name and passwords and stronger authentication, but we have also seen hybrids," he says, where hospitals have used a combination of passwords with smart cards. Smart Systems for Health did not comment for this story.

On a smaller scale, Ontario has done what Bush hopes to create in the United States. Last year the U.S. Department of Health and Human Services requested information from industry regarding a potential network that would link the 4,000 sub-networks that currently exist around regional health care centers.

The Liberty Alliance, a group of 150 companies working on a standard for online identification, recently responded to the request with a system that would ensure a patient's privacy by never storing the information in one place at any time.

For example, when a patient visits the doctor, both will authenticate themselves to the Web-based network. The doctor will be able to access the relevant parts of the medical record while the patient is present. But after he or she leaves the office the records "blow apart," says Michael Aisenberg, director of government relations at Mountain View, Calif.-based Verisign Inc., a security company that is a member of the Liberty Alliance.

Smart cards or other security technologies could be used to access the information on this new network, says Piper Cole, vice president of government and community affairs at Sun Microsystems. Stricter identification could be used when accessing secure areas of the network.

Two companies, Dallas-based HealthMeans Inc. and Moonachie, N.J.-based Competech Smart Card Solutions, are touting the benefits of smart cards for use in health care.

Frank Avignone, vice president at HealthMeans, says the company introduced its smart card system in August and is currently involved in six projects. One involves a community hospital with 150 beds and 80 physicians. After visiting the doctor a patient would have his or her information stored on the card and it would be updated upon every visit, he says.

The card could also be used to store prescription information, Avignone says. HealthMeans is currently negotiating with local pharmacies to have drug information stored on the smart card.

Pharmacies may be the first locations where smart cards find their niche with consumers, says John Ekers, product marketing director for software and services at Eden Prairie, Minn.-based Fargo Electronic. Some elderly patients might be taking multiple medications from various doctors. In order to make sure there are no harmful drug interactions, many patients carry all their medications with them to doctor's appointments.

A simple solution would be a prescription smart card that tracks all medication, Ekers says. "Just sharing basic prescription information is a nice, easy first step," he says. "It can be a transaction, just like a Visa card." <

> Images, Page 1

would be a departure from how biometrics have been typically stored on ID cards. Templates, or mathematical representations of the biometric, have generally been used because the file size is smaller, matching is quicker and to avoid privacy issues.

Already privacy advocates are expressing concerns about the choice to use images over templates. "The goal of interoperability shouldn't be set above security and privacy protection," says Pam Dixon, executive director of the World Privacy Forum, a nonprofit organization that studies technology and privacy. "At this point interoperability has been placed above those concerns."

'The goal of interoperability shouldn't be set above security and privacy protection. At this point interoperability has been placed above those concerns.'
— Pam Dixon, World Privacy Forum

While Wilson favors using images now, he says the spec could be updated later if testing shows that a standard template can be read by different vendors. NIST will be conducting such tests later this year.

And Wilson cautions that there is a chance that images may not work across agencies, depending on the matching algorithm that different departments choose. "Even starting with the same definition we don't know if it will work," he says. "One company could design a product that captures a small amount of minutia points while another company might want to gain a large number of minutia points." Minutia points are the spots that fingerprint algorithms map out to match images.

Outside of law enforcement or background checks it is rare that fingerprint images are used. Biometric deployments that allow an individual access to a computer network or to a secure facility have used templates because of file size and matching speed. Templates are about 200 hundred bytes, while fingerprint images are 17 times that size at about 7,500 bytes each, says Wilson.

Christophe Goyet, technical director for government and ID programs at Oberthur Card Systems Corp., says storage space on the smart card will not be an issue. The two fingerprint images will take up roughly 15 kilobytes of space, which leaves plenty of room on a 64K card, he says. Oberthur, the U.S. subsidiary of France-based smart card vendor Oberthur Card Systems, has been a supplier of smart cards to the U.S. Defense Department and other government agencies. The new smart card ID could eventually be issued to 7 million employees and contractors.

Others, however, question whether these relatively large image files will leave enough space on the card for agency-specific applications, such as a stored value feature. The Transportation Security Administration Worker Identification Credential is using a 64K smart card, and there are reports of memory constraints with that ID.

Using images may also drastically slow down the time to confirm a match using commonly available traditional biometric access control products, Wilson says. Extracting the image from the card, mapping out points on the stored image and then comparing it to the live image presented would take about 90 seconds, he says.

These readers commonly use technology that is the equivalent of a 200 megahertz processor, which were common on personal computers in the mid-1990s. Using templates, the match can be made in a matter of seconds, but processing the image requires more time, Wilson says.

There are vendors that could provide quicker matching, Wilson says. South Pasadena, Calif.-based Cogent Systems says it's one of them. Cogent has a reader that can perform the image match in seconds, says James Jasinski, executive vice president at the biometric firm. He echoes Wilson's interoperability concern regarding templates. "Based on the testing that's been done, interoperability with (templates) will be inconsistent," he says.

Speed might not be that great of a concern because the images would likely only be used in limited situations, such as when visiting another agency for the first time or for access to highly secure areas, Wilson says.

For example, if a government employee goes to another facility he or she would swipe the ID card, enter a six-digit PIN to unlock the fingerprint images on the card and then present their biometric for matching. Once a positive match is made, the employee would be on their way. "This is an interface that allows you to verify the identity of someone you have never seen before," Wilson says.

But the cost may be too high, according to some privacy activists. The concern is that the fingerprint image could be taken off the card, recreated and used maliciously, such as to gain unauthorized access to facilities or computer networks. While removing a fingerprint image from a smart card would be difficult, it is not impossible, says World Privacy Forum's Dixon. Templates are designed to be difficult to reverse engineer into the original image.

Ari Schwartz, associate director at the Washington-based Center for Democracy and Technology, says the benefit of using an image does not outweigh the risk. "While the risk of a breach is slim, the consequences are simply too high to risk the privacy and security of the federal workforce and beyond," he says.

The decision to use images could potentially delay the entire project and others like it because of the privacy fears, says Rob Atkinson, vice president of the Progressive Policy Institute and director of its technology and "new economy" project. "This sets a bad precedent," he says. "NIST has left some of the privacy issues unstated, and that leaves it open to the privacy zealots."

This biometric specification, Special Publication 800-76, is not the first controversy to come out of the move toward a standard government ID card, which was mandated by President Bush last August. NIST released a smart card specification in November that diverged from existing deployments and could have required existing programs to reissue millions of cards.

The Interagency Advisory Board, a group of U.S. government smart card experts, submitted its own draft of the smart card standard to NIST last week, and NIST is expected to release its revised version of the document in the next couple of weeks. Since the biometric spec also departs from traditional installations, some are looking to see how NIST responds to the concerns about the smart card standard for an indication of whether the agency will heed the concerns raised about the biometric proposal. <

> Menu, Page 1

rics to pay, no one knows which students are receiving subsidies. "Kids in the high school won't allow themselves to be labeled and don't sign up for the program," Johns says. "The doctor's kid who may have $500 in an account and the kid receiving the subsidized lunch go through the same process."

The biometric payments system also makes sure that only eligible students receive the free lunch. Students would be enrolled on the program before the start of the school year and have a fingerprint enrolled. The biometric makes sure that they are receiving the lunch and not having someone else use their ID or ticket.

"The use of biometric technology to discreetly keep track of which children are eligible for free or reduced-price lunches is significant since almost a billion dollars out of the $6.8 billion dollars of funding for the program went to buying lunches for ineligible children in 2002, according to the USDA," says Wong.

In the Penn Cambria school district in Pennsylvania, 1,817 students are enrolled at five schools, says Brenda Bucynski, secretary to the Penn Cambria School District food service director. The district decided to deploy the fingerprint system because of its security. "We wanted something each individual student had that somebody else couldn't copy," she says.

The district has eight fingerprint readers at the five school cafeterias, Bucynski says. The system has been in place since 1999, and students are enrolled when entering the school district.

The Wilson School District in Eaton, Pennsylvania, decided to go with biometrics after its "paper and pencil" prepayment system became too time-consuming, says Pat Anthony, food service director for the district. "The popularity of the prepayment program, however, exceeded our capabilities of managing the extensive paperwork," she says.

Parents would prepay for lunches and students would then receive a four-digit personal identification number that they would recite to a cashier after receiving the meal. Student receiving free lunches though the National School Lunch Program also received PINs to prevent overt identification. The program was entirely paper-based and every time a student prepaid the roster would have to be updated, copied and sent to the cashiers.

The biometric program is not mandatory for the 5,154 students in the district, but it is popular. "Enrollment and participation in the elementary areas is quite high, about 98% enrolled, with about 75% routinely using," Anthony says. "In the secondary areas, enrollment is about 80%, with 60% using routinely." The school has 25 scanners installed at the five schools.

Johns introduced the first fingerprint payment system in 1999 and initially found the technology was not as accurate as vendors claimed. But the accuracy has improved and the school is not having many issues with accuracy, he says. The system costs $5,000 per lane, Johns says.

Some parents are leery of a fingerprint system at first, Johns says. But he says the schools explain that the fingerprint image is not being stored, just a mathematical representation of the image, Johns says. That digitized version cannot be used to recreate the original finger image.

Student reaction has been positive and kids "like the high-tech concept," Johns says. <

Sagem Morpho provides the fingerprint POS readers used at the schools.

Advantages Of The Biometric Payment System

- **Accountability to parents & students.**
- **Enhances the perception of the department's credibility and capability.**
- **Streamlines collection of data for state and federal accountability reports.**
- **Well-documented paper trail for accounting audits.**
- **Reduces the need for students to carry cash to school.**
- **Prevents overt identification of students participating in the Free/Reduced lunch program.**

Source: Wilson School District

Implantable RFID Chip Takes Root in CIO... Literally

John Halamka, M.D., will always have a chip on his shoulder.

Halamka, chief information officer at Boston's CareGroup Healthcare System, is the first volunteer to test an implantable radio frequency identification chip for medical use. He had the grain-sized VeriChip, from Delray Beach, Fla.-based Applied Digital, implanted into his arm on Dec. 22.

The device was approved in October by the Food and Drug Administration for medical use in humans. Each VeriChip contains a 16-digit identification number assigned by the vendor. The number can be captured by waving the vendor's RFID VeriChip Pocket Reader over a patient with an implanted chip. The number can be linked to a database at a health care organization that contains a patient's medical information.

After Halamka met with VeriChip officials in November, he volunteered to evaluate the device and share his assessment with the vendor and the health care industry. He was implanted with the chip by an orthopedist at Beth Israel Deaconess Hospital, a CareGroup facility, in what he called a painless, 15-minute procedure. "The implantation required local anesthesia to a two-inch area of my arm between my elbow and shoulder," he explains. "The chip was inserted under my skin—between the fascia and the muscle. I can't feel it."

Nearly 40 people across the United States have been implanted with a VeriChip and are testing the device, says Richard Seelig, M.D., vice president of medical applications at Applied Digital. These volunteers, however, are using the system for identification and security access applications—not health care.

Potential Risks

The FDA identified several risks and recommended measures to mitigate the risks, which include: adverse tissue reaction, migration of the implanted responder, MRI incompatibility and needle sticks. To date, Halamka says he hasn't had any side effects, even after he was exposed to cold climates and high altitudes.

Halamka had his VeriChip number digitally mapped to his master patient index number at CareGroup. To assess the reliability of the chip, Halamka used the vendor's RFID reader to locate the chip and display its identification number. He then typed the identification number into the delivery system's Web-based master patient index to retrieve his medical information.

Halamka was able to retrieve an accurate reading of his chip's ID number by scanning up to 5 inches away. He also was able to retrieve it while his arm was covered with layers of clothing and apparel with metal.

He says the device could be used in future medical applications to retrieve information from a non-responsive patient and increase patient safety by verifying a medication or procedure was being given to the correct person. Halamka says he plans to keep the chip intact and hopes he will be able to use it in the future at other health care organizations.

"It's a permanent device, so its effectiveness won't change over time," he says. "I'm giving the industry a learning opportunity by testing it."

Privacy Issues

Some industry experts agree VeriChips could improve emergency care and patient safety by authenticating patients and caregivers. They also, however, say there are some weeds around the implantable chip that must be pulled before its use can grow in the industry. Ensuring privacy is one such issue, says Eric Brown, vice president at Cambridge, Mass.-based Forrester Research.

Though the VeriChips thus far do not contain any protected health information, there are other privacy concerns associated with the technology. For instance, their manufacturer could begin offering VeriChip readers to other industries. People implanted with the chip for medical purposes might not want other organizations, such as retail stores or restaurants, being able to identify them as they walk into their establishment, contends Claudia Tessier, executive director at the Washington-based Mobile Healthcare Alliance.

When other types of RFID technology, such as chip-enabled badges or pins, are worn by individuals, this signifies they are actively initiating their authentication. The VeriChip, however, is implanted, which means another person could initiate contact without an individual's consent. This raises the concern that the implanted individual could be unknowingly identified, Brown says.

Both Tessier and Brown maintain some sort of legislative agreement should be developed to ensure implanted individuals can stipulate when such chip technology can and can't be read.

While Halamka's chip currently only can be read at CareGroup, that soon could change. The provider organization is taking part in a statewide initiative to develop a Massachusetts health information network. The network will offer data exchange and electronic medical records systems interoperability--which eventually could enable access to Halamka's chip by other provider organizations across the state.

Applied Digital will begin marketing the VeriChip system to clinicians and provider organizations this month, Seelig says. It will be classified as a prescription medical device and require a physician to perform the implantation. The vendor will sell the chips to patients for $200 and the readers to health care organizations for $650, Seelig adds. The cost of implantation will be established by a patient's physician. <

— By Beckie Kelly Schuerenberg, senior editor at Mobile Health Data and Health Data Management, sister publications of IDNewswire.

IDNewswire®
Trends in Personal Identification and Biometrics

Editor
Zack Martin
zachary.martin@thomsonmedia.com

Group Editor
Donald Davis
don.davis@thomsonmedia.com

Contributing Editor
Kevin Woodward
kevin.woodward@thomsonmedia.com

Advertising Sales
Jim Baker
james.baker@thomsonmedia.com

Publisher
Andrew Rowe
andrew.rowe@thomsonmedia.com

Thomson Media: *James M. Malkin, Chairman & CEO; William Johnston, Chief Financial Officer; Celie Baussan, Senior Vice President, Operations; Robert DeNoia,Vice President, Human Resources; Bruce Morris, President, Banking & Corporate Group; Frank Quigley, President, Securities Group; Heather O'Leary, Vice President of Marketing & Communications*

IDNewswire® is published twice monthly by Thomson Media. Visit our Web site at http://www.cardtechnology.com. The contents of IDNewswire are, and remain, the property of Thomson Media. Reproduction or forwarding of this publication is strictly prohibited. Individuals who infringe on these rights will be prosecuted to the full extent of the law. IDNewswire is a registered service mark used herein under license.

Subscribers who want multiple copies of IDNewswire should contact Barbara Mahin at 212-803-8768 or barbara.mahin@thomsonmedia.com for information. The annual subscription rate is $695. For subscription, renewal or licensing information, please contact Barbara Mahin at 212-803-8768 or barbara.mahin@thomsonmedia.com.

For advertising information, contact Jim Baker at 312-983-6179 or james.baker@thomsonmedia.com. Editorial offices are located at 300 S. Wacker Drive, 18th Floor, Chicago, IL 60606. Telephone: 312-983-6168. FAX: 312-913-1365.

IBG: Why Biometrics Makes Sense In Mobile Phones

The following is an edited transcript of the January teleconference by Jim Chou, a consultant with the New York-based International Biometric Group.

As cell phones become more feature-rich and essential to our daily lives, the importance of securing these devices becomes more important. Evolving from boxy and cumbersome sets used solely for voice communication, the cell phone is almost a misnomer today – a tool that not only makes voice calls, but sends text messages, browses the web, schedules meetings, and plays music.

More and more financial transactions are conducted on cell phones, thus necessitating some form of user authentication. Cell phones are also innately personal; while a traditional land line phone usually reaches a household or an entire office, almost every individual has his or her own cell phone. For these reasons, and others discussed later, biometric utilization has been and will be a relevant force in the cell phone industry.

Consumer Desire

The drive for biometrics in cell phones is two-fold: not only is there an inherent technical need, but there is also a consumer desire. According to a survey conducted by StrategyOne in November, 71% of consumers would pay additional money for fingerprint biometrics in their cell phones.

Respondents indicated a desire for mobile commerce and wireless banking; 60% expressed a desire to replace their wallets with biometrically-equipped cell phones, to purchase items from a store, execute wireless banking or access mass transit.

Further substantiating this study is a separate survey commissioned by EDS and the International Association of Privacy Professionals, which found that only 12% of those questioned were against biometrics as a form of identity verification.

This study also found that a primary driver for the incorporation of biometrics in cell phones is the compelling convenience they provide. Instead of remembering passwords and PINs or carrying a hefty wallet of credit cards, individuals would be able to take advantage of a single device to accomplish these tasks with the assurance and security provided by biometric protection.

Market Demand By Region

The advent of biometrics in cell phones has been of consequence primarily in Asia followed by Europe, the typical progression of cell phone technology. U.S. industry regulations are habitually more stringent, as high-tech devices normally debut here anywhere from a few months to a couple of years after their counterparts in Asia and Europe.

'Instead of remembering passwords and PINs or carrying a hefty wallet of credit cards, individuals would be able to take advantage of a single device to accomplish these tasks with the assurance and security provided by biometric protection.'

The market for cell phones is drastically different in Asian countries, such as Japan and Korea, than in the United States. In Asia, cell phone manufacturers are separated from service providers. The device producers are thus inclined to develop and include new features, like biometric security, to increase sales. However, with a limited number of service providers controlling the models being sold in the United States, features filter out more slowly. Current projections place biometric cell phones entering the American market by the end of 2006.

A number of other factors contribute to the disparity in market emergence. Third-generation, or 3G, mobile telephony network protocols, are networks that allow higher-bandwidth data transfers. They are now fully deployed in many Asian and European countries, but will not be in the U.S. mainstream for at least a year.

International Data Corporation of Japan projects over 69 million Japanese subscribers in 2007 using the 3G networks. The additional bandwidth can be used for a myriad of functions, from accessing company networks to transferring personal pictures to video-conferencing. Ensuring security for these transactions is increasingly vital.

Additionally, European cellular users have shown greater concern about mobile network security and identity theft. Proponents of biometrics in cell phones stress that the benefits not only expedite customer utility, but also ease merchant fraud liability. Finally, since most cell phones store irreversible templates instead of actual images, privacy concerns are assuaged.

> IBG, Page 8

Drivers For Biometric Cell Phones

Technical Need: Additional authentication needed for better security.

Consumer Desire: 71% of consumers say they would pay additional money for fingerprint biometrics in their cell phones.

Convenience: Instead of remembering passwords and PINs, individuals would be able to make transactions with a single device.

> IBG, Page 7

Fingerprint Recognition Technology

The specific biometric most widely used today in cell phones is fingerprint recognition technology. Silicon sensors, which use silicon chips, have been popular for integration, due to their small form factor, low cost and modest power requirements. Next-generation sensors have durable, scratch-resistant surfaces and are touted to be resilient against the hazards of daily cell phone use. Silicon sensors are also not affected by imperfections such as dirt or oil on the skin.

A second and older type of sensor, the optical sensor, is also prevalent. Optical sensors are built of hard, coated plastic or glass. Both silicon and optical sensors have varying form factors on cell phones, from full surface area platens down to small swipe sensors, where the finger is moved over a small sensor strip.

'The need for biometrics in cell phones is clear, and consumer demand, especially in Asia and Europe, is dictating the rapid inclusion of these various technologies. Whether it is to store secret phone numbers, or act as a credit card, biometrics is facilitating the ever-expanding functionality of the cell phone.'

The swipe sensor is used in a recently introduced Korean cell phone, for example. The inclusion of a fingerprint sensor is especially critical for this particular phone, given that it offers a music player with stereo speakers, a built-in camera, GPS locator, and mobile banking capabilities.

While these devices are all relatively new, the industry is still constantly seeking novel ways to improve the technology. A Japanese computer company, for example, has developed a prototype fingerprint sensor layered on top of an LCD screen, combining the phone's display and biometric security into a single, space-saving component. Form factor is critical; however, it is the accuracy of matching and the protection of identity that validates the use of biometrics. Fingerprints have proven to be largely effective in this regard.

Voice Verification

Another technology used currently in cell phones is voice verification, possibly the most natural biometric extension.

Voice verification requires no additional hardware – the requisite microphone is already present. When dealing with voice verification, there are two distinct implementations related to cell phones.

The first is directly analogous to what a fingerprint biometric provides – the unlocking of features, services and data on a particular mobile device. This usually involves initially storing a custom voice pass-phrase on the phone, and repeating this pass-phrase to enable service.

The second and more prevalent use of voice verification is using automated voiceprint technology in the phone system itself, rather than the physical handset. This has been deployed in certain financial services organizations in the United States, to ensure that customers seeking to secure transactions or access privileged records are whom they claim to be.

This latter implementation of voice verification does not require a cell phone; a land line works as well. However, as telephony applications are quickly converging with wireless networking, cell phones are becoming the primary client for these systems. To this end, voice verification products in development often address and compensate for the lower quality of sound that cell phones produce.

Facial recognition

Facial recognition rounds out the existing implementations of biometrics in cell phones. Much like voice verification, facial recognition technology is able to leverage existing infrastructure – a digital camera.

Analysts estimate that 650 million cell phones with built-in cameras will be sold in 2008, up from 150 million in 2004. Like other biometrics, facial recognition will permit users to safely protect private data as well as conduct financial transactions. For example, a California-based facial recognition company has developed software successfully operable on cell phones to authenticate purchases.

The law enforcement sector has also used facial recognition in cell phones to its advantage. A Chicago-based company has launched phones that can pick out faces in a field of view and search them against known criminals. Upon finding a match, the system then sends an alert to the officer's mobile phone. Finally, in Japan, several phones not only provide verification and security through facial recognition, but also determine their users' changing expressions, displaying special effects such as tears when a sad face is recognized.

Iris Recognition

Iris recognition has potential as a biometric solution for cell phone security. As it stands today, iris recognition is comparatively cost-prohibitive and requires a relatively steep measure of user habituation. However, the accuracy of iris recognition has been repeatedly enforced as the technology continues to improve and, ultimately, iris recognition also allows for hands-free operation similar to facial recognition. An upcoming iris recognition deployment will involve a mobile camera that attaches to a PDA, storing images on a secure digital card.

The need for biometrics in cell phones is clear, and consumer demand, especially in Asia and Europe, is dictating the rapid inclusion of these various technologies. Whether it is to store secret phone numbers, or act as a credit card, biometrics is facilitating the ever-expanding functionality of the cell phone.

Analysts have also predicted cell phones in the travel and transportation arena, using them to check in for a flight, select a seat via text messages, and automatically resolve any needed rebooking. Cell phones will conceivably serve as ticket and boarding passes, or as fare for public transportation.

Already in Japan today, airport check-in identity can be verified using mobile phone straps embedded with a smart card chip holding facial and iris data. With production and deployment costs consistently decreasing and with cell phones becoming a critical part of personal and financial interactions, biometrics and cell phones will continue to evolve. <

For more information contact Chou at jchou@biometricgroup.com or 212-809-9491.